DUMPSBOSS.

Mist AI - Specialist (JNCIS-MistAI)

Juniper JN0-451

Version Demo

Total Demo Questions: 11

Total Premium Questions: 110

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Mist AI Features and Functionality	13
Topic 2, Wireless Assurance	77
Topic 3, Wired Assurance	1
Topic 4, Marvis Actions	9
Topic 5, Location Services	7
Topic 6, Premium Analytics	1
Topic 7, Mix Questions	2
Total	110

QUESTION NO: 1

Which two statements are true about 802.1X/EAP? (Choose two.)

A. Credentials are exchanged with a RADIUS server prior to the 4-way Handshake.

B. Credentials are exchanged with a RADIUS server after the 802.11 Association.

C. Credentials are exchanged with a RADIUS server after the 4-way Handshake.

D. Credentials are exchanged with a RADIUS server prior to the 802.11 Association.

ANSWER: A B

Explanation:

In an enterprise wireless network using 802.1X, a client first completes 802.11 discovery and association with the access point. Association establishes the basic wireless connection, but it does not yet grant normal network access. The client, acting as the supplicant, then uses EAPOL to exchange EAP authentication messages with the access point, which acts as the authenticator. The access point relays the applicable EAP information to the RADIUS authentication server. Therefore, credentials are exchanged with the RADIUS server after 802.11 Association.

After the RADIUS server successfully authenticates the client, WPA or WPA2/WPA3-Enterprise keying material is made available for the wireless security process. The client and access point subsequently perform the 4-way Handshake to derive and install the transient encryption keys that protect unicast traffic. Consequently, the RADIUS credential exchange necessarily occurs prior to the 4-way Handshake. This ordering separates identity authentication and authorization from the later establishment of data-encryption keys. Juniper's documentation describes 802.1X as an EAP-based authentication mechanism that uses a RADIUS server, while the Wi-Fi Alliance explains that enterprise Wi-Fi authentication precedes secure session key establishment. See Juniper 802.1X Authentication documentation and Wi-Fi Alliance security overview.

QUESTION NO: 2

What are two ways to access Marvis? (Choose two.)

A. Use the conversational assistant.

B. Use Actions.

C. Use Insights.

D. Use config templates.

ANSWER: A B

Explanation:

Marvis is accessed through the conversational Marvis Assistant and through Marvis Actions. The conversational assistant provides a natural-language interface where administrators can ask operational questions about users, devices, applications, and network behavior. Marvis interprets the question, correlates relevant telemetry, and returns context-specific answers to speed troubleshooting and operational investigation. Marvis Actions is the proactive operational interface for Marvis: it presents identified issues, their likely root causes, affected scope, and recommended remediation actions. This lets administrators begin from AI-driven findings rather than requiring a manually phrased question. Together, these interfaces support both reactive investigation through an interactive conversation and proactive review of AI-detected network issues. Juniper describes Marvis as an AI-native virtual network assistant and documents Marvis Actions as the location for viewing and acting on identified network problems. See the Juniper Marvis overview and the Marvis Actions documentation.

QUESTION NO: 3

Which Wireless Assurance SLE provides information on whether a user is able to associate to the WLAN?

A. Successful Connect

B. Capacity

C. Roaming

D. Throughput

ANSWER: A

Explanation:

Successful Connect is the Wireless Assurance service-level expectation that evaluates whether a wireless client can successfully join the WLAN. The client connection workflow includes discovering the network, associating with the access point, completing authentication when security is enabled, and obtaining network connectivity through DHCP. Successful Connect presents the success rate for these client connection attempts and supplies failure-stage visibility, allowing administrators to determine whether an unsuccessful connection occurred during association or another part of the join process. This makes it the appropriate SLE for answering whether a user is able to associate to the WLAN, as well as for investigating the conditions affecting that outcome.

In Mist Wireless Assurance, SLEs translate client and network telemetry into measurable user-experience indicators. Successful Connect is specifically focused on the initial process of getting a client connected, rather than performance after the connection is established. Its associated insights and event details help isolate connection-stage problems and identify affected clients, APs, SSIDs, and locations. Juniper documents the Successful Connect SLE and its connection-stage metrics in the Successful Connect SLE documentation; additional Wireless Assurance SLE context is available in the Wireless Assurance documentation.

QUESTION NO: 4

What does Mist's patented 16-element vBLE Antenna Array do when "engagement" is enabled?

A. performs radio resource management

B. locates Wi-Fi assets

C. transmits unique and directional BLE beams

D. performs personal pre-shared key sharing

ANSWER: C

Explanation:

When engagement is enabled, Mist’s patented 16-element virtual Bluetooth Low Energy antenna array transmits unique, directional Bluetooth Low Energy beams. This capability is designed to support location-aware mobile engagement: rather than emitting a single omnidirectional Bluetooth signal, the access point can create directional virtual Bluetooth Low Energy beams that mobile applications can use to determine a user’s proximity and direction relative to the access point. The directional nature of these transmissions enables highly targeted interactions, such as presenting relevant information, offers, navigation guidance, or other context-sensitive content to a mobile device based on its physical location. Juniper describes the virtual Bluetooth Low Energy capability as part of its access-point platform for precise indoor location and engagement services, with the antenna array enabling directional beam transmission. This function is distinct from general wireless management; its purpose under engagement is to provide the directional Bluetooth Low Energy signaling needed by location-aware experiences. See Juniper’s wireless access point portfolio and its virtual Bluetooth Low Energy documentation for additional product and feature details.

QUESTION NO: 5

Click the Exhibit button.

Referring to the exhibit, in the USA, which two statements are correct? (Choose two.)

A. The WLAN with SSID Eero1234 is not configured to industry best practices.

B. The WLAN with SSID Eero1234 is configured to industry best practices.

C. The WLAN with SSID NETGEAR24 is not configured to industry best practices.

D. The WLAN with SSID NETGEAR24 is configured to industry best practices.

ANSWER: A D

Explanation:

The WLAN with SSID Eero1234 is not configured to industry best practices, while the WLAN with SSID NETGEAR24 is configured to industry best practices. The distinction is determined by applying the United States regulatory domain and accepted WLAN channel-planning practices to the radio settings shown in the exhibit. A WLAN deployment must use channels and operating parameters permitted in its country of operation; in the United States, Wi-Fi operation is governed by FCC rules. Regulatory-domain compliance is foundational because access points and clients must operate only on frequencies authorized for that location. In addition, an effective WLAN design selects valid channels and channel widths that support predictable client connectivity while minimizing co-channel and adjacent-channel interference. The NETGEAR24 configuration shown in the exhibit aligns with those US requirements and design principles, whereas Eero1234 does not. Mist administrators should ensure that an organization, site, and access point are assigned the appropriate country code so that the permitted channel set and transmit-power constraints are applied correctly. See the FCC's Part 15 rules for unlicensed radio-frequency devices and Juniper's country-code configuration documentation.

QUESTION NO: 6

What is meant when a Marvis Action is shown as "AI Validated"?

A. The issue which triggered an alert has been set to Resolved status.

B. Marvis has observed a new issue.

C. Marvis has observed a recurring issue.

D. Marvis has observed an issue that is no longer present.

ANSWER: D

Explanation:

"Marvis has observed an issue that is no longer present." is correct. An AI Validated Marvis Action reflects Marvis's continuous analysis of network telemetry and client experience data: it detected the condition underlying an action, then subsequently observed that the condition ceased occurring. This status provides confidence that the issue was transient or has been remediated in the network, without requiring an administrator to manually establish that conclusion solely from individual events or alerts.

Marvis Actions are designed to prioritize and contextualize issues using AI-driven correlation, helping operators focus on conditions that affect users and infrastructure. The AI Validated state is therefore specifically about Marvis validating through later observations that the originally detected problem is no longer active. It is not merely a manually assigned lifecycle state; it represents an outcome derived from Marvis's ongoing visibility into the environment. This distinction helps network teams identify actions whose associated symptoms have cleared and assess whether any further operational follow-up is necessary. Juniper Mist's description of Marvis Actions and their action states is available in the Marvis Actions documentation. Additional product context is available on the Marvis AI page.

QUESTION NO: 7

Once a client discovers an access point, what is the correct order of steps for successful 802.1X authentication?

A. Open System Authentication -> 802.1X Authentication -> Association

B. Association -> 802.1X Authentication -> Open System Authentication

C. Association -> Open System Authentication -> 802.1X Authentication

D. Open System Authentication -> Association -> 802.1X Authentication

ANSWER: D

Explanation:

Open System Authentication -> Association -> 802.1X Authentication is the correct sequence because 802.11 network access begins with the client completing the baseline 802.11 management exchanges with the access point. After discovery through scanning, the client performs Open System authentication, which is the initial 802.11 authentication transaction used by modern WPA2/WPA3 enterprise WLANs. The client then sends an association request and, once the access point accepts it, becomes associated at the 802.11 MAC layer. Only after that association is established can the controlled port process the 802.1X/EAP exchange. The client, acting as the supplicant, exchanges EAPOL frames with the access point, which acts as the authenticator and relays authentication information to the configured RADIUS server. On successful EAP authentication, keying material is established and the client is authorized for protected network traffic. This ordering is important when troubleshooting enterprise WLAN joins: a failure before association is an 802.11 connectivity or management-frame issue, while a failure after association may involve EAP, certificates, user credentials, RADIUS reachability, or authorization policy. Juniper's overview of WLAN authentication is available in the Juniper WLAN authentication documentation; the underlying port-based access-control standard is maintained by the IEEE 802.1X working group.

QUESTION NO: 8

Your customer added an Apple TV in their conference room so that employees can easily share their screen. However, the Apple TV cannot be discovered by the employees' devices.

Which two settings are causing the problem? (Choose two.)

A. MDNS

B. Broadcast/Multicast

C. Ignore Broadcast SSID Probe Requests

D. ARP

ANSWER: A B

Explanation:

Apple TV discovery for AirPlay depends on Bonjour, Apple's implementation of multicast DNS (mDNS). The Apple TV advertises its available AirPlay services through mDNS multicast announcements, and employee devices use mDNS queries to locate those advertised services. Therefore, the **MDNS** setting must be enabled and correctly configured for the relevant WLAN or network segments so that clients can receive or relay Bonjour discovery traffic. Apple's Bonjour deployment guidance describes mDNS as the mechanism devices use to discover services such as AirPlay: Apple Platform Deployment: Bonjour deployment.

The **Broadcast/Multicast** setting is also required because discovery traffic is delivered using multicast. If multicast handling is disabled, suppressed, or configured in a way that prevents the required multicast frames from reaching wireless clients, the Apple TV's service advertisements and the clients' discovery queries will not be exchanged successfully. In a Mist WLAN, review the WLAN's multicast and service-discovery-related configuration, along with the network path between the Apple TV and employee devices. Juniper's Mist documentation provides WLAN configuration guidance at Juniper Mist Wi-Fi WLAN documentation.

QUESTION NO: 9

You are deploying multiple Mist APs across many sites in your network. You must ensure that you apply consistent WxLAN and WLAN policies across all sites within the same organization.

Which configuration object should be used to accomplish this behavior?

A. site labels

B. an RF template

C. a device profile

D. a config template

ANSWER: D

Explanation:

A config template is the appropriate organization-level object for consistently applying wireless configuration across multiple Mist sites. It provides a reusable, centrally managed configuration definition that can be assigned to sites, allowing the same WLAN settings and associated wireless policies to be deployed repeatedly without manually recreating them at each location. This standardization is particularly valuable in a multisite deployment because changes can be made in the shared template and then propagated to the sites using it, helping maintain a uniform service definition, operational posture, and user experience.

Config templates are intended to reduce configuration drift while still allowing an organization to scale its AP deployment across branches, campuses, or other locations. Administrators can organize common WLAN-related settings in the template and apply the template wherever the same design is required. Juniper's Mist documentation describes the configuration and management capabilities available for Mist Wi-Fi deployments, including reusable configuration constructs for site operations. See the Juniper Mist Wi-Fi configuration templates documentation and the Juniper Mist access point product information.

QUESTION NO: 10

What are two functions of Mist Radio Resource Management (RRM)? (Choose two.)

A. transmit power control

B. WLAN scheduling

C. channel assignment

D. Ethernet configurations

ANSWER: A C

Explanation:

Mist Radio Resource Management (RRM) optimizes the RF environment by automatically managing key radio parameters across the wireless network. **transmit power control** is an RRM function because the APs can adjust their transmit power in response to the surrounding RF conditions. Appropriate power levels help maintain usable client coverage while limiting unnecessary cell overlap, co-channel contention, and interference between neighboring APs. **channel assignment** is also a core RRM function. Mist can evaluate channel utilization and interference conditions, then select or recommend channel assignments that make better use of the available spectrum. This dynamic RF management is especially valuable as client density, neighboring networks, and sources of interference change over time.

Mist describes its RRM capabilities as using AI-driven analysis to optimize RF operations, including channel and transmit-power decisions. These controls support reliable connectivity and improved capacity without requiring administrators to manually tune every AP radio. Juniper's Mist Wi-Fi documentation and product materials provide further detail on the platform's RF optimization and automated operations: Juniper Mist Wi-Fi Assurance and Mist Wi-Fi Documentation.

QUESTION NO: 11

Which 802.11 management frame is transmitted periodically by an AP to advertise the presence and capabilities of a WLAN?

A. Beacon

B. Probe request

C. Acknowledgment

D. Clear to Send

ANSWER: A

Explanation:

Beacon is correct. An AP periodically transmits beacon frames to advertise its basic service set (BSS). A beacon can include information such as the SSID, BSSID, supported data rates, security capabilities, channel information, and timing data.

Wireless clients can use beacon information during passive scanning to identify available WLANs and evaluate whether they can join them. Probe requests and probe responses are used during active scanning, while acknowledgments are control frames used to confirm frame receipt. See the IEEE 802.11 Working Group for IEEE 802.11 standards information.